

ADAPTIVE METHOD FOR AMORTIZING

AUTHENTICATION OVERHEAD

→ This application claims benefit of Provisional 60/230,301, filed 09/06/2000, also Claims claims benefit of Provisional 260/230,319, filed 09/06/2000.

FIELD OF THE INVENTION

The invention relates generally to network security and, more particularly, to the field of authentication.

BACKGROUND OF THE INVENTION

There are two major areas of the art of networking security, encryption and authentication. Encryption is a method of hiding or encrypting the data in transmission so that only the recipient may have access to the data in its unhidden or unencrypted form. This is also known as data privacy. Authentication on the other hand is a method of ensuring that a transmission that is sent from a sender to a receiver in fact came from the true sender. This is otherwise known as integrity. A method that provides encryption ensures that only the appropriate and intended receiver may possess the method to decrypt the data for use, and a method that